How Technology Drives Vehicular Privacy

ALEECIA M. MCDONALD & LORRIE FAITH CRANOR*

ABSTRACT

Technological changes in the past twenty years have contributed to decreased privacy in privately owned vehicles in the United States. This paper presents six areas in which new technologies have privacy-invasive aspects that many people fail to fully appreciate: "black boxes" ("EDRs") in cars, traffic cameras, OnStar, GPS transponders attached to cars, EZ-PASS (an RFID-based highway toll system), and proposals for new "use taxes" based on where and when people drive. This survey is useful in understanding the cumulative effect of new technologies, rather than just examining each in isolation.

I. INTRODUCTION

The public is largely unaware of the potential for privacy invasion that rides along with the newest gadgets in their cars. This paper provides information about how newer automotive technologies work, what they were originally designed to do, and the additional privacy-invasive purposes new technologies may be used for. These additional purposes often come as a surprise to car owners.

Many papers discussing threats to privacy tend to focus on one issue at a time; for example the risk of a "black box" in a car that tells police the driver's speed prior to a car crash. This paper catalogs a variety of different technologies and the threats they present. In addition to the convenience of one paper that summarizes several major threats to vehicular privacy, this approach also emphasizes just how much privacy we have lost - in many cases, with little or no public debate.

Cellular phones pose their own set of privacy concerns. Uncertain regulatory rules spawned industry guidelines on location-based services.[1] While people in cars can be tracked by their cell phones, we see this as an issue that happens to overlap with traveling in a car, rather than an issue specific to vehicular privacy. As such, we do not address cell phones specifically in this paper. With that said, we

---

* Aleecia M. McDonald is a PhD candidate in Engineering & Public Policy at Carnegie Mellon University; Lorrie Faith Cranor is an Associate Research Professor in the Computer Science and Engineering & Public Policy departments of Carnegie Mellon University.

[1] Linda Ackerman, James Kempf, Toshio Miki, "Wireless Location Privacy: Law and Policy in the U.S., EU and Japan," *The Internet Society (ISOC) Member Briefing*, no. 15 (2003), http://www.isoc.org/briefings/015/index.shtml.

would be remiss if we did not note that cell phones can be used to track traffic congestion, which is a use of cellular technology specific to vehicular privacy. For example, the Missouri Department of Transportation plans to use cell phone location data to track traffic conditions on 5,500 miles of major roads.[2]

In this paper, we first summarize the legal context for vehicular privacy in the United States. This is particularly relevant in understanding how law enforcement and government agencies can obtain and use information.

Next we turn to technology issues in six areas: black boxes in cars, traffic cameras, OnStar, GPS transponders attached to cars, EZ-PASS, and other RFID-based highway toll systems, and highway use tax proposals. Again, these areas are specifically limited to implementations in the United States.

In conclusion, we look at the types of privacy threats posed by each of the six technologies, and we consider how those technologies can be combined to erode privacy even further.

II. AUTOMOTIVE PRIVACY IN THE UNITED STATES

A. LEGAL ENVIRONMENT

While there is no right to privacy explicitly codified in the United States Constitution, the Fourth Amendment does provide some protection:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[3]

While people have some expectation of privacy in their own homes, courts have narrowed privacy rights with regard to cars since

---

[2] David A. Lieb., "Mo. May Track Cell Phones for Traffic Data," *ABC News*, October 14, 2005, http://abcnews.go.com/Technology/wireStory?id=1214736.

[3] U.S. CONST. Amend. IV.

the Supreme Court ruled in *Carroll v. U.S.* in 1925[4] - only seventeen years after the introduction of the Model T.[5]

FindLaw's annotated Fourth Amendment provides a good overview of the legal context.[6] Reasons for a reduced expectation of privacy in cars include the following.

- The difficulty for a police officer to obtain a warrant to search a car before it moves. Therefore, in some cases no warrant is required.[7]
- Cars travel on "public thoroughfares where both its occupants and its contents are in plain view."[8]
- The contents of a car may not be private either[9] — police can search a closed suitcase or a glove compartment without a warrant after they have arrested the driver on unrelated charges.[10]

More recently, the Supreme Court upheld a ruling in *Illinois v. Caballes* that police can conduct a search based on a dog sniffing drugs in a car - even when there is no probable cause to bring the dog to the car. Justice Stevens' reasoning included his view that there is no expectation of privacy for illegal activities.[11] Further case law may determine if speeding is likewise an illegal activity that bars expectations of privacy.

---

[4] *Carroll v. U.S.*, 267 U.S. 132 (1925).

[5] Ford Motor Company, "History," http://www.ford.com/en/heritage/history/default.htm.

[6] FindLaw, "U.S. Constitution: Fourth Amendment: Annotations," http://caselaw.lp.findlaw.com/data/constitution/amendment04/03.html#f55.

[7] *Carroll*, 267 U.S. at 153.

[8] *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974).

[9] *Rakas v. Illinois*, 439 U.S. 128, 148-49 (1978).

[10] *Colorado v. Bertine*, 479 U.S. 367, 370 (1987).

[11] Michael C. Dorf, The Supreme Court upholds suspicionless dog sniffs, *FindLaw*, February 1, 1999, http://writ.news.findlaw.com/dorf/20050201.html.

In general, the Supreme Court has ruled in favor of law enforcement's interest to search cars over the car owner's privacy interests. Consequently, some privacy advocates have largely given up on the courts. Instead, they look to solutions from regulatory boards, new legislation, or new technologies.

B. COMMON CHARACTERISTICS OF PRIVACY THREATS

Many specific vehicular privacy invasions are comparatively new and have come about as a result of changes in technology. However, at a more general level, the backdrop for vehicular privacy threats looks much the same as other categories of privacy loss. There are two main concerns: mission creep and deliberate abuse.

Privacy advocates warn of "mission creep:"[12] the government (or private corporations) collect data for one purpose, but once they have the data they find new ways to use it. For example, New York introduced Metrocards for the subway system to replace tokens and allow riders to use one payment method across transit types. Within a month of installing Metrocard stations in subways, the police used Metrocard data to track a suspect.[13] More recently, the FBI told Congress that the PATRIOT Act is important in part because now the FBI can track people by their electronic highway toll payment system without waiting for judicial oversight.[14]

Certain technologies also have multiple primary purposes. For example, some cities have both red light cameras and cameras to measure traffic flow. These are different systems with different goals. This is not a case of cameras being used in secondary ways; there are multiple primary purposes for cameras pointed at vehicular traffic.

In addition, there is the potential for deliberate abuse of the data collected. IRS employees comb through the tax files of celebrities,

---

[12] Lieb, "Mo. May Track Cell Phones for Traffic Data," (see n. 2).

[13] New York City Transit - History and Chronology, *Metropolitan Transit Authority, State of New York*, http://www.mta.nyc.ny.us/nyct/facts/ffhist.htm; Adam L. Penenberg, "The Surveillance Society," *Wired Magazine*, December 2001, http://www.wired.com/wired/archive/9.12/surveillance.html.

[14] Valerie Caproni, General Counsel for the Federal Bureau of Investigation, testifying before the Senate Select Committee on Intelligence, *Bill to Reauthorize Certain Provisions of the U.S.A. Patriot Act and for Other Purposes*, 109th Cong., 1st sess., May 24, 2005, http://intelligence.senate.gov/0505hrg/050524/caproni.pdf (testimony regarding toll systems was during question and answer session).

prospective dates, neighbors, as well as people critical of them - including people who did nothing more than write letters to the editor.[15] Even when it is illegal to browse files, as it is for IRS employees, abuse remains a risk. This risk increases when systems collect more personal information than they need, and when information is stored indefinitely.

It is human nature to use the tools we have. Sometimes that leads to new uses for existing data, and sometimes it leads to abuse. We recommend designing systems with mission creep and abuse in mind and thinking about ways to mitigate risks prior to launching new systems.

III. SIX TECHNOLOGIES CONSIDERED

We consider six technologies that may affect vehicular privacy. Five have already been deployed; highway "use taxes" are still in the proposal stage. After discussing each in turn, we summarize the privacy threats they pose.

A. BLACK BOXES

Many people are familiar with the phrase "black box" in the context of airplanes - devices that record the conditions in the aircraft right before a crash.[16] Many cars have similar black boxes, also known as Event Data Recorders ("EDRs").[17] As of May, 2005, about 25 million cars in the United States had EDRs.[18] Most people do not know if they have an EDR in their car. About two-thirds of Americans do not even know cars can have EDRs at all.[19]

---

[15] Prepared Statement of Witness Before the Senate Finance Committee, *Oversight Hearing on the Internal Revenue Service,* 105th Cong., 1st sess., September 25, 1997, http://enzi.senate.gov/anon3.htm.

[16] Minutes of the Nevada Senate Committee on Transportation and Homeland Security, 73rd sess., May 10, 2005, http://www.leg.state.nv.us/73rd/Minutes/Senate/TRN/Final/4454.pdf(hereinafter Nevada Senate Committee).

[17] John G. Spooner, "Rocky Road for Car 'Black Boxes,'" *CNET News.com*, March 9, 2005, http://news.com.com/Rocky+road+for+car+black+boxes/2009-1041_3-5604449.html.

[18] Nevada Senate Committee (see n. 16).

[19] Associated Press, "Evidence From Black Boxes in Cars Turns Up in Courts," *FOXNews.com*, June 28, 2003, http://www.foxnews.com/story/0,2933,90673,00.html.

1. HOW EDRS WORK

EDRs sit under the front seat of a car and collect information from the car's systems.[20] EDRs are usually installed at the time a car is manufactured, but there are also after-market EDRs that can be installed.[21]

Cars moved from mechanical systems to electronic systems about twenty years ago. Electronic systems monitor different parts of a car with a set of sensors. An Electronic Control Unit ("ECU") collects information from sensors, processes the information, and sends instructions to various subsystems. EDRs capture electronic information and store it for a brief amount of time.[22]

Different EDRs capture different data. EDRs vary by automobile model, and newer EDRs generally capture more data than early EDRs. EDRs usually store less than ten seconds of data, frequently far less.[23]

2. ORIGINAL USE

United States car makers began to install primitive EDRs in the late 1970s, with more sophisticated versions in the last 1990s. Car makers used EDRs to collect data after crashes and to improve car safety. They answered the following questions. Did the airbag deploy as designed? Did someone step on the gas instead of the brake?[24] Car manufacturers were able to this type of access data when people brought cars to the dealership for repairs.[25]

---

[20] The Volpe National Trasportation Systems Center, "Highlights," The Volpe National Trasportation Systems Center, March/April 2004, http://www.volpe.dot.gov/infosrc/highlts/pdf/03-0404.pdf.

[21] Ibid.

[22] Julian Edgar, "Logging Your Every Driving Moment," *Silicon Chip Online*, November 17, 2003, http://www.siliconchip.com.au/cms/A_30802/article.html.

[23] Ibid.

[24] Spooner, "Rocky road for car 'Black Boxes,'" (see n. 17).

[25] Bob Gritzinger, "Under the Hood, with Big Brother," *AutoWeek*, November, 8 2004, http://www.autoweek.com/apps/pbcs.dll/article?AID=/20041108/FREE/411080714.

3. NEW USES

Today, EDRs are used in several ways:

- **Understanding accidents.** Data from EDRs can be used to make cars safer. For example, if people hit the gas when they meant to hit the brakes, it suggests an opportunity to redesign the car's layout.[26]

- **Court cases, particularly to establish excessive speed.** The star witness in many cases has been data from EDRs. In most cases it has been used to find a driver guilty, but in at least one case it has been used to establish innocence.[27]

- **Monitoring teens.** A commercial product taps into EDRs to signal drivers that they are cornering too hard, driving too fast, or braking too aggressively. It emits a clicking tone that gets progressively louder if the driver's behavior doesn't change. It also logs data from EDRs, which allows parents to find out if their teens have driven the family sedan in excess of the speed limit.[28]

- **Insurance companies.** Most drivers have insurance, thus court cases often involve two companies fighting it out to determine liability.[29] In addition, Progressive Insurance had a pilot program

---

[26] Associated Press, "NTSB wants black boxes in passenger vehicles," *FOXNews.com*, August 3, 2004, http://www.foxnews.com/story/0,2933,127945,00.html.

[27] David Hechler, "Pandora's High-tech Boxes Hit the Courts," *The National Law Journal*, October 20, 2003, http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1066080441829; Associated Press, "Evidence From Black Boxes in Cars Turns Up in Courts," (see n. 19); Harris Technical Services, "EDR Case Law," http://www.harristechnical.com/cdr5.htm.

[28] Spooner, J. "Rocky road for car 'Black Boxes,'" (see n. 17).

[29] Progressive Auto Insurance, "Black Box a Reality Big Brother is Here! - Progressive to Use Data-Logging Device," *The Auto Channel*, August 9, 2004, http://www.theautochannel.com/news/2004/08/09/208150.html.

> that offered discounted rates to "good drivers" who turned over EDR data that they stored on a second chip that customers mailed back to Progressive. Discounts were offered for people who drove lower distances, drove at particular times, and drove under seventy-five miles per hour.[30]

Data on EDRs is particularly relevant in legal cases with fatal crashes. Excessive speed can be used to support a contention of negligence; a jury could find a speeding driver was not acting within the reasonable person standard. For speeds in excess of twenty miles per hour over the speed limit,[31] some states apply a strict liability standard,[32] which holds the driver at fault for whatever else occurs even if the driver would not otherwise be found to have intentionally or negligently committed a crime.[33]

Insurance is probably the second most important use of EDR data. As the Los Angeles Times reports, "already there are private sector plans to collect a huge pool of accident data from the recorders with the aim of finding more cost-effective ways to service insurance claims and simplify litigation. That sounds good, too, on the face of it. But emerging technologies have a way of beginning as one thing and then oozing Blob-like into something else."[34]

---

[30] Dawn Love, "Progressive's Black Box: Is Big Brother Good for the Industry," *Insurance Journal*, December 6, 2004, http://www.insurancejournal.com/magazines/southeast/2004/12/06/features/50322.htm.

[31] *District of Columbia v. Colts*, 282 U.S. 63, 73 (1930) "An automobile is, potentially, a dangerous instrumentality, as the appalling number of fatalities brought about every day by its operation bear distressing witness. To drive such an instrumentality through the public streets of a city so recklessly 'as to endanger property and individuals' is an act of such obvious depravity that to characterize it as a petty offense would be to shock the general moral sense. If the act of the respondent described in the information had culminated in the death of a human being, respondent would have been subject to indictment for some degree of felonious homicide."

[32] See, e.g., Va. Code. Ann. § 46.2-862(2004).

[33] Daniel N. Steven, "Negligence primer," *publishlawyer*.com, 2001, http://www.publishlawyer.com/negligen.htm.

[34] Salley Shannon, "Witness on Board," *The Los Angeles Times Magazine*, July 17, 2005, http://www.latimes.com/. The article is also available at the following source: Salley Shannon, "Witness on Board," *Garrett Engineers, Inc.*, http://www.garrett-engineers.com/mambo/index.php?option=com_content&task=view&id=52&Itemid=82.

4. LEGISLATION AROUND BLACK BOX DATA

The National Transportation Safety Board ("NTSB") initially opted not to get involved in recommendations over EDRs in cars, stating that it liked how the industry was progressing without any new regulation. However, in 2004 the NTSB reversed its stance and called for mandatory EDRs, along with a standard set of data that must be collected.[35]

As a report for the National Cooperative Highway Research Program concludes, legal issues around rules of evidence are not a strong concern:

> although the data (and the recorder itself) may be "owned" by the automobile's owner or lessee, that data may almost certainly be used as evidence against that owner (or another driver) in either a civil or criminal case. Certainly nothing within the Federal Rules of Evidence (FRE) or the Fifth Amendment's protection against compelled self-incrimination would exclude the use of data recorded by the EDRs . . . . the issue here is not one so much of legal authority to use EDR data in court, but instead what the public will accept . . . the problem is less a legal concern than it is a battle to mold public perception.[36]

More specifically, EDR data is admissible in court under the *Daubert* test, since it "possesses the requisite scientific validity to establish evidentiary reliability."[37] In a privacy-friendly move, California passed a state law in 2004 to require car manufacturers to disclose black boxes by mentioning them in car manuals. Further, the law states that car owners also own the data on their EDRs.[38] California's law has become a model for legislation in other states.[39]

---

[35] Associated Press, "NTSB Wants Black Boxes in Passenger Vehicles," (see n. 26).

[36] Hampton C. Gabler et al., *Use of Event Data Recorder (EDR) Technology for Highway Crash Data Analysis*, (December 2004), 119-20, http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_w75.pdf.

[37] Ibid., 160.

[38] Hechler, "Pandora's High-tech Boxes Hit the Courts" (see n. 27).

[39] Nevada Senate Committee (see n. 16).

Arkansas, Nevada, North Dakota, and Texas enacted similar legislation in 2005. Eleven other states also considered legislation in 2005, but failed to pass laws during the 2005 session.[40] As of August, 2006, a total of twenty states have introduced legislation.[41]

There are minor variations between the state laws. All five carve out an exception that EDR data may be used without consent to perform medical research on crash reactions.[42] North Dakota is unique in specifically barring insurance companies from using EDR data to set insurance rates.[43] Arkansas' law is fairly typical in granting ownership of the data to car owners, yet specifies that the data can be used without the owner's consent in several ways - such as by a court, a police officer with probable cause, the Highway and Transportation Department to calculate fuel taxes or mileage, and EDR data may be entered into any civil or criminal court case if "relevant and reliable."[44]

Data ownership does not appear to curtail facing your car as the star witness in a court case against you. It remains to be seen in practice how these new state laws will change the legal landscape.

Insurance companies are frustrated by the new laws, because they need either the owner's permission or a court case to gain access to data. In states with EDR laws, insurance companies cannot use data accessed during car repairs to deny a claim, or raise a customer's rates. However, at least one car repair center has provided EDR data directly to insurance companies.[45] New state laws also make it more difficult

---

[40] National Conference of State Legislatures, "2005 Legislation Related to Event Data Recorders ("Black Boxes") in Vehicles, http://www.ncsl.org/programs/lis/privacy/blackbox05.htm.

[41] National Conference of State Legislatures, "2006 Legislation Related to Event Data Recorders ("Black Boxes") in Vehicles," http://www.ncsl.org/programs/lis/privacy/blackbox06.htm.

[42] S.B. 51, 85th Gen. Assembly (Ark. 2005); A.B. 315 (Nev. 2005); S.B. 2200, 59th Leg. Assembly (N.D. 2005); H.B. 195 (Tex. 2005); CAL VEH. CODE 9951 (2006).

[43] S.B. 2200, 59th Leg. Assembly (N.D. 2005).

[44] David Reddick, "Regulating Event Data Recorders: How Should Insurers React to New State Laws?," *NAMIC* Online, July, 2005, 2 http://www.namic.org/insbriefs/050722BlackBox.pdf.

[45] Charles Baker, "Black Box FAQs," *Collision Repair Industry INSIGHT*, November, 2005, http://www.collision-insight.com/news/archives/200511-feature.htm.

for insurance companies to charge rates based on mileage.[46] Researchers are looking at the economic implications of a system called pay-as-you-drive-and-you-save ("PAYDAYS") to determine how to tie insurance rates to mileage.[47]

5. PRIVACY CONCERNS

If consumers tamper with the EDRs in their cars, they will also interfere with the signals that tell air bags to deploy or car seat belts to adjust during a crash.[48] Because seat belts are mandatory, it may be illegal to attempt to disable EDRs. In Montana, New Hampshire, and New Jersey, new bills would explicitly give owners permission to turn off EDR data collection, even though it means disabling the airbags in the process.[49]

Privacy advocates are frustrated that in most states, car owners do not know EDRs are in their cars, consumers do not have the choice to turn off EDRs, and there are no guidelines limiting who can access EDR data or what it can be used for.[50]

EDRs pose several risks. EDRs are seen as evidence rather than self-incrimination which can give rise to criminal and civil liability. EDRs also pose the risk of adverse insurance policy changes.

B. TRAFFIC CAMERAS

Traffic cameras evolved from a system designed by race car driver Maurice Gatsonides; frustrated by inaccuracies from stop watches, Gatsonides developed a series of automated ways to time cars.[51]

---

[46] Reddick, "Regulating Event Data Recorders: How Should Insurers React to New State Laws?" (see n. 44).

[47] Allen Greenberg, "Applying Mental Accounting Concepts in Designing Pay-Per-Mile Auto Insurance Products," *Federal Highway Administration, Office of Policy*, November 21, 2005, http://www.mdt.mt.gov/research/docs/trb_cd/Files/06-2976.pdf.

[48] Shannon, "Witness on Board," (see n. 34).

[49] Baker, "Black Box FAQs," (see n. 45).

[50] Kelley Beaucar Vlahos, "Privacy Experts Shun Black Boxes," *FOXNews.com*, September 10, 2004, http://www.foxnews.com/story/0,2933,132056,00.html.

[51] Ross Finlay, "Gatso and the Cameras," *ITV*, May 10, 2001, http://www.itv-motoring.com/columns/ross_finlay/1510.asp.

Red light cameras take photographs of cars that run red traffic lights. They catch both cars that continue through the intersection after a yellow signal, and cars that edge into the intersection before the light turns green. The reduced cost and size of video cameras, which is a key factor in adoption. Red light cameras were introduced in the United States over forty years ago, however it has become pervasive only in the last ten years.[52]

Traffic cameras are also used in a variety of contexts other than monitoring red lights. They are used to measure speed and issue speeding tickets. Many cities use cameras to monitor traffic flow. This way they can find more efficient routes for emergency vehicles, and can adjust traffic signals to better handle congestion, for example, after a football game.[53]

1. HOW TRAFFIC CAMERAS WORK

Systems vary widely. A typical red light camera system works with roadway sensors that communicate with traffic lights.[54] When a car enters an intersection while the light is red, the sensor sends a message to a camera.[55] The camera captures an image of the car in the intersection.[56] Cameras are usually mounted high above the road, and generally operate in pairs to confirm that the car crossed into the intersection.[57] Cameras bathe the intersection in an electronmagnetic field which allows their operation to trigger upon the presence of a violating automobile.[58] The cameras then send the images to a central computer for processing.[59]

---

[52] Tom Harris, "How Red-light Cameras Work," *HowStuffWorks*, http://electronics.howstuffworks.com/red-light-camera6.htm.

[53] Michael Learmonth, "Say Cheese," *Metroactive*, February 6, 1997, http://www.metroactive.com/papers/metro/02.06.97/traffic-camera-9706.html.

[54] Harris, "How Red-light Cameras Work," (see n. 53).

[55] Ibid.

[56] Ibid.

[57] Ibid.

[58] Ibid.

[59] Ibid.

Different systems capture different levels of detail. At minimum, systems capture the vehicle's license plate.[60] In the early days of red light cameras, a clerk would look at the picture of the license plate, look up the registration information for the vehicle, and send a ticket to the owner.[61] Today, the process is typically contracted out to a firm that uses image-processing software to automatically process the image and determine the license plate.[62] The license plate number can then either be sent to the municipality to look up in a computer database, or municipalities can grant access directly to registration databases.[63] Some systems still use film rather than digital cameras.[64] In that case, a worker must go to each camera to collect the negatives and install new film.[65]

Most cameras show the make, model, and color of the car.[66] Cameras record the time and date the image was taken.[67] Because cameras are usually used in pairs, it is generally possible to calculate a vehicle's speed.[68]

Even though most cameras are infrared, it is usually possible to determine the race of the driver and any passengers. Less common, some systems also use image recognition software to identify drivers and passengers; automated facial recognition is used in security systems to grant access to corporate parking lots.[69]

---

[60] Yoram Hofman, "License Plate Recognition - A Tutorial," May 2, 2004, http://www.licenseplaterecognition.com.

[61] Ibid.

[62] Ibid.

[63] Ibid.

[64] Matt Labash, "Inside the District's Red Lights," *The Daily Standard*, April 1, 2002, http://www.weeklystandard.com/Content/Public/Articles/000/000/001/078ftoqz.asp?pg=2.

[65] Ibid.

[66] Learmonth, "Say Cheese," (see n. 53).

[67] Ibid.

[68] Ibid.

[69] Hofman, "License Plate Recognition - A Tutorial," (see n. 60).

2. ORIGINAL USES

Traffic cameras were presented as a way to enhance safety. Some of the reasons given for installing cameras include the following

- Red light cameras act as a deterrent for running red lights, thus pre- venting accidents.[70]
- Speed trap cameras act as a deterrent against excessive speed, again preventing accidents.[71]
- Video cameras in police cars document officers' conduct, which de- creases police brutality.[72]
- Traffic cameras monitor the flow of traffic on highways and main roads to help emergency vehicles find the fastest route to an accident. They also help reduce congestion, because traffic signals can be adjusted to respond to conditions.[73]

3. NEW USES

Red light cameras capture images of crashes. These images can be used to determine which driver was at fault.[74]

Red light cameras are a substantial revenue source for local governments. Washington, D.C.'s red light camera system generated

---

[70] "Digital enforcement for speeding and red light," Institute for Traffic Care, http://www.itctraffic.com/camera.htm.

[71] Ibid.

[72] Jim Herron Zamora, "Oakland Cops May Go to Video; City Wants Cameras in Police Cars," *The San Francisco Chronicle*, February 2, 2004, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/02/02/BAGOA4MSAC1.DTL&hw=video+camera&sn=052&sc=203.

[73] Learmonth, "Say Cheese," (see n. 53).

[74] TheNewspaper.com, "The Red Light Running Crisis: Is it Intentional?", May 2001, http://www.thenewspaper.com/rlc/reports/rlcreport6.asp.

$18 million in tickets from 1999 to 2002.[75] D.C.'s photo radar system (automated fines for speeding) made $9 million in its first seven months of operation.[76] While raising funds from people who break the law is not necessarily a bad thing, there are concerns that local governments are installing red light cameras strictly as a source of profit, rather than out of concern for citizens' well-being.

Red light cameras were supposed to reduce accidents because fewer people would run lights. However, there is evidence to show that red light cameras cause accidents: drivers slam on their brakes to avoid tickets, which leads to an increase in rear-end collisions in intersections that have red light cameras. In some cases, while rear-end collisions increase, more dangerous T-bone accidents decrease.[77] However, the details appear to vary widely. For example:

- Fort Collins, Colorado had an 83% increase in accidents,[78]
- Portland, Oregon had a 140% increase in rear-end collisions,[79]
- The Washington, D.C. area had more than twice as many accidents, and fatal crashes increased 81%.[80]

---

[75] Erin Mahoney and Joanne Helperin, "Caught! Big Brother May Be Watching You With Traffic Cameras," *Edmunds.com*, October 28, 2004, http://www.edmunds.com/ownership/driving/articles/42961/article.html.

[76] Labash, "Inside the District's Red Lights," (see n. 64).

[77] Del Quentin Wilber and Derek Willis, "D.C. Red Light Cameras Fail to Reduce Accidents," *washingtonpost.com*, October 4, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/10/03/AR2005100301844.html.

[78] TheNewspaper.com, "Colorado Study: Red Light Cameras Increase Accidents 83 Percent," October, 30 2005, http://www.thenewspaper.com/news/07/740.asp.

[79] Anna Song, "Do Red Light Cameras Pose Safety Problems?", *KATU News*, November 11, 2005, http://72.14.209.104/search?q=cache:m2NTeKEiEI0J:www.katu.com/printstory.asp%3FID%3D81073+%22do+red+light+cameras+pose+safety+problems%22&hl=en&gl=us&ct=clnk&cd=2.

[80] Wilber & Willis, "D.C. Red-light Cameras Fail to Reduce Accidents," (see n. 77).

There is a simple way to decrease the number of people who run red lights: lengthen the time the light is yellow. The Institute of Transportation Engineers ("ITE") decreased their recommended yellow light length by as much as a third since the 1970s recommendations.[81] Yellow lights were once four to six seconds long, and are now typically three to four seconds.[82] Eighty percent of motorists who run red lights do so in the first second the light turns red - time when it would still be yellow under the older guidelines.[83] The ITE suggests that instead of longer yellows that allow drivers to react, thanks to traffic cameras, "enforcement can be used instead."[84]

While local governments vigorously deny they are motivated by money rather than safety, it does seem that money factors into decisions. For example, Fort Collins increased the length of yellow lights and saw such a large decline in revenues that they decided to hold off installing new red light cameras, out of fear they might lose money.[85] In Washington, D.C., camera placement did not correlate with the intersections with the greatest number of accidents. Instead, contractors helped the city identify intersections likely to generate the greatest number of infractions and profits.[86] Similar placement trends have been documented in Charlotte, North Carolina and San Diego, California. Intersections at the bottom of hills with yellow lights of three seconds or less are particularly popular.[87]

4. PRIVACY CONCERNS

Perhaps the most alarming use of traffic cameras is illustrated in China. Cameras used to measure traffic congestion around Tiananmen Square provided images which the Chinese government broadcasted

---

[81] Matthew Labash, "The Yellow Menace," *The Daily Standard*, April 2, 2002, http://www.weeklystandard.com/Content/Public/Articles/000/000/001/079bkyhi.asp?pg=2.

[82] Ibid.

[83] Ibid.

[84] Ibid.

[85] TheNewspaper.com, "Colorado Study: Red Light Cameras Increase Accidents 83 Percent," (see n. 78).

[86] Labash, "The Yellow Menace," (see n. 81).

[87] Ibid.

on TV, and helped them round up student leaders who had escaped the 1989 massacre.[88] Today, China is installing more cameras in the Tibet Autonomous Region.[89] The stated reason is that cameras are used to track traffic congestion, even though several areas where they are installing cameras have only pedestrian traffic.[90]

In the United States, there is no law that mandates municipalities need a data retention policy. It is entirely possible that images could be archived for years, then sifted through with facial recognition software to retroactively determine the movements of a person of interest.

Because cameras send photos of the front seat occupants along with a ticket, there have been several reports of red light cameras leading to marital strife. The Cato Institute commented on the story of a woman "who got in hot water when an intersection camera caught her joyriding in her husband's pet sports car - a car he'd forbidden her to drive."[91] Extramarital affairs may also be discovered by traffic photos enclosed with tickets.

Privacy concerns have been cited in decisions not to install cameras, or to remove them. Usually it is accompanied by another reason - for example, privacy and a lack of revenues with longer yellow lights, or privacy and concern that police officers would lose jobs.[92]

C. GPS TRANSPONDERS

Global Positioning System ("GPS") transponders use a system of twenty-four satellites to calculate precise world-wide locations in three dimensions (latitude, longitude, and height).[93]

---

[88] Greg Walton, "China's Golden Shield: Corporate Complicity in the Development of Surveillance Technology," *Human Rights in China*, June 17, 2002, http://www.hrichina.org/public/contents/article?revision%5fid=2440&item%5fid=2439.

[89] Ibid.

[90] Ibid.

[91] Radley Balko, "Not So Candid Camera," *The CATO Institute*, February 6, 2002, http://www.cato.org/research/articles/balko-020206.html.

[92] The Highway Safety Group, "Red Light Camera Timeline 2002," http://www.hwysafety.com/nma_rlc_timeline4.htm.

[93] RadioShack Corporation, "A Guide to the Global Positioning System (GPS)," http://support.radioshack.com/support_tutorials/gps/gps_hist.htm.

GPS alone just calculates position. However, GPS is frequently combined with transmitters that send the data to a receiver, or with media (like a hard drive, or a USB flash drive) to capture data for later retrieval.

1. HOW GPS TRANSPONDERS WORK

GPS transponders can determine their precise location by bouncing signals off of satellites.[94] The satellites have atomic clocks, and calculate time very accurately.[95] GPS was conceived shortly after Sputnik's launch.[96] Scientists realized that since they could track Sputnik's signal and figure out where it was in space, the converse must be true: they can use signals to satellites in space to determine location on earth.[97] GPS transponders use multiple signals from satellites to triangulate position.[98]

2. ORIGINAL USE

GPS is a military technology. It was used, and is still used, for troop deployments, supply drops, and bomb targeting.[99]

3. NEW USES

The United States government allows anyone to use the signal from GPS satellites, free of charge. Thus, a wide range of applications developed.[100] Early uses were for ships' navigation.[101] Currently,

---

[94] Ibid.

[95] Ibid.

[96] Ibid.

[97] Ibid.

[98] Ibid.

[99] RadioShack Corporation, "A Guide to the Global Positioning System (GPS)," (see n. 93).

[100] Scott Pace et al., "National Interests and Stakeholders in GPS Policy," in *The Global Positioning System: Assessing National Policies* (Santa Monica: The RAND Corporation, 1996), http://www.rand.org/pubs/monograph_reports/MR614/MR614.sec2.pdf, 12.

[101] Ibid., 12.

some computer networks use the time from GPS satellites to ensure they keep time accurately and uniformly[102] while surveyors use GPS to determine the exact location of property lines.[103]

In automobiles, GPS systems are coupled with map services to show drivers where they are. These systems are advertised as enhancing safety, because lost drivers do not have to "struggle with a large map" or "ask a stranger for directions."[104] However, a study by Privilege Insurance found that GPS-based map systems are more distracting than paper maps.[105] Further, people who own GPS-based map systems are more likely to just start driving without looking for directions first.[106]

General Motors is testing a new system that uses both GPS and a communications system to allow all similarly equipped cars to communicate.[107] The goal is to avoid car crashes.[108] This system is seen as an improvement over existing radar systems since it is not affected by fog, rain, or snow.[109]

4. PRIVACY CONCERNS

Law enforcement uses GPS to automatically track a suspect's car through one of two ways. Police can affix a GPS device to a car, usually hidden underneath and held to the car frame with a magnet, and then return later to retrieve the device and the data. Or, police can use a GPS transponder to broadcast location data in real time. The first

---

[102] Ibid., 15.

[103] Ibid.

[104] "iGuidance Intelligent GPS Navigation," MightyGPS.com, http://www.mightygps.com/triptracer/iguidance.htm.

[105] Reuters, "Report: In-Car Navigation Systems Can be Dangerous," *ZDNet News*, February 21, 2006, http://news.zdnet.com/2100-1035_22-6041393.html.

[106] Ibid.

[107] Jim Mateja, "GM System Lets Cars Talk to Each Other," *Navigadget*, February 4, 2006, http://www.navigadget.com/index.php/2006/02/04/gm-system-lets-cars-talk-to-each-other.

[108] Ibid.

[109] Ibid.

GPS case led police to a nine-year-old's body in 2003.[110] National attention focused on this issue as part of the media coverage of the Peterson murder trial, when the court upheld its use .[111]

Courts have held that because GPS functions as an automated replacement for "tailing" a car, it comes under no more judicial oversight. Initially, probable cause was not required.[112] However, the Washington State Supreme Court has since ruled that a warrant is necessary, which in turn necessitates a determination of probable cause.[113]

As of February 2006, the Los Angeles police department is currently testing a system that allows them to fire GPS darts at moving cars. "Each unit can fire two GPS tracking devices containing a battery and a radio transmitter embedded in an epoxy compound. The tag affixes to the suspect's vehicle and transmits its location via satellite to police headquarters. The system is approved by the National Security Agency."[114]

GPS could be widely deployed on vehicles for an entire community, such as all members of a political or religious group. The records can be saved and matched against other people's data retroactively, for example as part of social network analysis.

GPS could also be used to alert a community about an individual's location. For example, GPS could be used to inform neighbors about a former sex offender's current location. Individuals can even use GPS to spy upon each other. Divorce lawyers and private investigators advertise their use of GPS data to potential clients.[115]

---

[110] Associated Press, "Cops Challenged on GPS Use," *Wired News*, May 21, 2003, http://www.wired.com/news/privacy/0,1848,58948,00.html?tw=wn_story_related.

[111] Rusty Dornin, "Judge Allows GPS Evidence in Peterson Case," *CNN.com*, February 17, 2004, http://www.cnn.com/2004/LAW/02/17/peterson.trial/.

[112] Associated Press, "Cops Challenged on GPS Use," (see n. 110).

[113] American Civil Liberties Union, "In Landmark Ruling, Washington Supreme Court Says Police Need Warrant for Surveillance with Global Tracking Devices," September 11, 2003, http://www.aclu.org//privacy/spying/14888prs20030911.html.

[114] Nadja Brandt, "Los Angeles Turns to GPS Devices to End Deadly Police Chases," *Bloomberg.com*, February 21, 2006, http://www.bloomberg.com/apps/news?pid=10000103&sid=aYPV2SPTS9.o&refer=us.

[115] Ben Stevens, "GPS Trackers Foil Cheating Spouses," *South Carolina Family Law Blog*, August 7, 2005, http://www.scfamilylaw.com/divorce-46-gps-trackers-foil-cheating-spouses.html.

D. ONSTAR

OnStar is a commercial service that alerts the police when cars are in accidents, and offers consumer convenience benefits for a monthly fee. Initially an optional service, since 2004 it has been pre-installed on most General Motors cars. It will be mandatory in all General Motors cars from 2007 forward.[116] Mercedes-Benzes, BMWs, and Jaguars use a similar technology to perform the same functions.[117]

1. HOW ONSTAR WORKS

OnStar's strength is that it combines the use of many different technologies. OnStar combines GPS transponders for vehicle tracking, a hands-free voice activated cell phone to talk to OnStar employees, and real-time monitoring of data from the car's EDR. OnStar employees can open doors or turn off car engines without being physically present.[118]

2. ORIGINAL USE

OnStar was promoted as a safety feature. It can track when airbags deploy, call the cell phone in the car to check for false alarms, and notify the police if appropriate. OnStar was also advertised as a roadside assistance program, and its advertising frequently depicts the service saving people in peril.[119]

3. NEW USES

Because OnStar is always on, its data is valuable to law enforcement. The company does require a warrant before it grants

---

[116] OnStar, "OnStar and StabiliTrak To Become Standard Equipment on GM Vehicles," http://www.onstar.com/us_english/jsp/new_at_onstar/onstar_standard_2007.jsp.

[117] Shannon, "Witness on Board," (see n. 34).

[118] OnStar, "OnStar Vehicle Diagnostics," http://www.onstar.com/us_english/jsp/ovd/index.jsp (accessed September 21, 2006).

[119] Ibid.

access to its databases, and explicitly states that it maintains that policy out of fear it will lose customers over privacy concerns.[120]

OnStar realized that with the data it already collects, it can tell how many passengers are in a car. It can also tell the passengers' weight from data it collects to suppress airbags in certain crashes. Using this data, and data concerning the region of a car that was hit during an accident, OnStar can calculate how likely it is that someone is badly injured. This lets the company prioritize calls to emergency services. One of OnStar's engineers was quoted in the press saying, "This is a great secondary use."[121]

4. PRIVACY CONCERNS

Privacy experts from the Electronic Frontier Foundation ("EFF") and the Electronic Privacy Information Center ("EPIC") voiced concerns that the tracking data OnStar collects could be used in unexpected ways. One example they offer: if OnStar records show you stopped at a bar for three hours, might that be entered into evidence in a court case, even if you never had a drink while you were there?[122]

OnStar has been used to catch drunk drivers.[123] One driver pushed the OnStar button repeatedly, failed to respond to inquires, and was subsequently arrested after the OnStar employee called the police to report the vehicle's location.[124] Regarding the situation, a state police sergeant summed it up, "[s]ometimes, you get help that you didn't expect."[125]

Even law makers are surprised when they realize the scope of data collected by OnStar. A state Senator in North Dakota was quoted as

---

[120] Robert Block, "In Terrorism Fight, Government Finds a Surprising Ally: FedEx," *post-gazette.com*, May 26, 2005, http://www.post-gazette.com/pg/05146/510879.stm.

[121] Rachel Konrad, "Car-Tracking System: Promises, Potholes," *ZDNet News*, August 1, 2002, http://news.zdnet.com/2100-9595_22-947519.html.

[122] Ibid.

[123] Susan Field, "OnStar Leads Police to Drunken Drivers, *The Morning Sun*, August 1, 2002. http://www.themorningsun.com/stories/120205/loc_onstar001.shtml.

[124] Ibid.

[125] Ibid.

saying "[w]hen I bought my car, I didn't realize that I was also buying a highway patrolman to sit in the back seat."[126]

The FBI realized that systems like OnStar can be turned on at any time, even if a consumer does not pay for the service. They used this feature to surreptitiously monitor all conversations in a car. The Ninth Circuit Court of Appeals ruled against the FBI's use of a system similar to OnStar,[127] although not because it was invasive of privacy, but because the FBI wiretap interfered with the basic functionality of the system.[128] If there had been an accident, the system would not have worked. Federal law enforcement can listen in via OnStar and related technologies without notice, even for people who are non-subscribers, so long as they structure the system so that OnStar remains operative. It stands to reason they could listen in on non-subscribers at any time, because they will not disrupt the functionality of a system that is not in service.[129]

The website onstarprivacy.com details several privacy concerns including the following.

- Progressive Insurance has a pilot program to give "good driver" discounts based on OnStar data. The concern is car insurance companies will require data access as a condition of insurance.[130]

- Data may be for sale or shared between the General Motors family of companies.[131] Will dealerships decide you abused your car and it is now out of warranty?

---

[126] Shannon, "Witness on board," (see n. 34).

[127] *The Company v. USA*, 349 F.3d 1132, 1146 (9th Cir. 2003).

[128] Kevin Poulsen, "Court Limits In-car FBI Spying," *The Register*, November 20, 2003, http://www.theregister.co.uk/2003/11/20/court_limits_incar_fbi_spying.

[129] *See* Ibid.

[130] Onstarprivacy.com, "Boycott All GM Vehicles with OnStar," http://www.onstarprivacy.com.

[131] Ibid.

- Progressive Insurance offers discounts to Progressive customers who allow Progressive Insurance access to black box data.[132] GMAC Insurance offers a twenty percent discount for customers who subscribe to OnStar.[133] Again, the concern is eventually all insurance companies will demand data as a condition of insurance.

- OnStar launched a "Virtual Advisor" service.[134] It was designed to announce where to find inexpensive gas when OnStar senses your fuel gauge is low.[135] It can also push ads that match location-based information with user profiles; for example, to tell an avid golfer that she is three blocks away from a sale on golf clubs.[136] Not everyone is comfortable with the idea of merchants purchasing location data for advertising. For instance, imagine driving with a child in the back seat as an ice cream shop offers a discount – or what magazines might arrive in the mail based on which shop you parked in front of.

E. E-ZPASS

E-ZPass and several similar systems are used to pay highway tolls automatically. Drivers put a small transmitter in their car, and funds are automatically deducted each time they drive through a toll both.

---

[132] Hampton C. Gabler et al., *Use of Event Data Recorder (EDR) Technology for Highway Crash Data Analysis* (Transportation Research Board of the National Academies, 2004), http://trb.org/publications/nchrp/nchrp_w75.pdf, 136.

[133] OnStar, "GMAC Insurance Discount," http://www.onstar.com/us_english/jsp/explore/onstar_extras.jsp

[134] Rachel Konrad, "General Motors to 'Push' Ads to Drivers," *CNET News.com*, January 8, 2001, http://news.com.com/2100-1023-250696.html?legacy=cnet.

[135] Ibid.

[136] Ibid.

1. How E-ZPass works

The underlying technology is Radio Frequency Identification ("RFID"), which sends a radio signal to a receiver.[137]

E-ZPass uses a semi-passive RFID tag. All E-ZPass tags have a non-replaceable lithium battery, which limits the life of the tag to two to five years.[138] E-ZPass communicates by taking an incoming radio signal from an RFID reader, and bouncing back a modified signal that contains the ID number for the device. As a result, E-ZPass can only "speak when spoken to" — it cannot broadcast information unless a reader requests it. This differs from GPS devices, which often contain transmitters that send real-time updates of location.

2. Stated Purpose

E-ZPass bills itself as a convenient, easy, and fast way to pay tolls.[139] Some highways have special lanes reserved just for motorists with E-ZPass. Because cars pass through toll booths more quickly, E-ZPass may also reduce pollution and save fuel.[140]

3. New Uses

E-ZPass is primarily used for paying tolls on highways, though the data does find its way into other uses. The customer agreement takes into account situations when the pass itself may be used in other ways: "[n]or are we liable for any third party act taken by reason of your use or display of the E-ZPasstag."[141]

---

[137] Kelly Shermach, "Legoland RFID Tracks Lost Kids, Collects Data," *CRM Buyer*, October 28, 2004, http://www.crmbuyer.com/story/Legoland-RFID-Tracks-Lost-Kids-Collects-Data-37694.html.

[138] Maine Turnpike Authority, "E-ZPass Information - Frequently Asked Questions," http://www.ezpassmaineturnpike.com/info/faqs.html#q21.

[139] Federal Highway Administration, "Excellence in Highway Design - E-Z Pass Electronic Toll Collection Program," http://www.fhwa.dot.gov/eihd/ezpass.htm.

[140] Ibid.

[141] New Jersey Customer Service Center, "E-ZPass Private Agreement Terms and Conditions," http://www.ezpass.com/static/terms/i_terms.pdf.

E-ZPass is used to pay for airport parking in Pittsburgh, New York, New Jersey, Texas, Chicago, and Delaware.[142] Drivers take parking tickets when they enter, and at exit have a choice of paying with cash, credit, or debit from their E-ZPass account.[143]

While a few McDonald's on Long Island allow drive-thru customers to pay with E-ZPass, it has not proven economically successful to the point of justifying installing E-ZPass hardware in more McDonald's locations.[144]

Transcom uses E-ZPass to assess traffic conditions in New York, New Jersey, and Connecticut.[145] Transcom installed roadside readers along the I-95 corridor to read E-ZPass tags.[146] It can measure how many cars go past. If the number of cars passing a reader suddenly drops, there must be congestion before the reader. Transcom scrambles the E-ZPass ID code so it can obtain data without tracking individuals.[147]

4. PRIVACY CONCERNS

Because E-ZPass transponders only provide information when they are scanned, they are less privacy-invasive than GPS, which captures location information all the time. Still, E-ZPass data has shown up in surprising contexts. For example, E-ZPass data has been used in divorce cases to support allegations of infidelity.[148]

Additional E-ZPass scanners could be placed along local roads to track traffic off highways as well as on them. Furthermore, because RFID technology broadcasts a signal to anyone with a scanner, it

---

[142] TOLLROADSnews, "E-ZPass Plus Flies at New York Area Airports," May 13, 2004, http://tollroadsnews.info/artman/publish/article_485.shtml.

[143] Ibid.

[144] Ibid.

[145] Carolyn S. Konheim, "Intelligent Transportation Systems in the New York Region: An Overview," *TransportLink*, Winter 1998-1999, http://transport-link.com/region/ITSOverview.htm.

[146] Ibid.

[147] Ibid.

[148] Shermach, "Legoland RFID Tracks Lost Kids, Collects Data," (see n. 137).

would be fairly easy for a stalker to track a target leaving home or work every time.

The FBI cited E-ZPass data as one example of data they can obtain without judicial oversight, and used it as an argument in favor of keeping all USA PATRIOT Act provisions.[149] Law enforcement is also interested in E-ZPass data to track suspects and missing persons.

Drivers are concerned that E-ZPass will eventually be used to issue speeding tickets. It is easy to calculate an average speed over the distance between two tollbooths. While stories abound of "a friend of a friend" getting a ticket in this way, it does not appear that E-ZPass is currently being used to issue speeding tickets.

F. HIGHWAY "USE TAX" PROPOSALS

Several states, most notably Oregon[150] and California, are investigating "use tax" to replace gasoline taxes. The idea is that as people buy more hybrids, gasoline taxes will decrease, which leaves states short on funds to maintain roads.[151] Instead, proponents suggest a new tax based on miles driven and time of travel. For example, driving during rush hour might cost consumers more than driving at three a.m., due to the higher volume of traffic during the former time.

1. HOW "USE TAX" COULD WORK

The most complete proposal involves a government-mandated GPS transponder that tracks everywhere a car travels, then sends a bill

---

[149] Caproni, *Bill to Reauthorize Certain Provisions of the U.S.A. PATRIOT Act and for Other Purposes*, (see n. 14). The testimony regarding toll systems was during the question and answer session.

[150] Examples abound. *See* Road User Fee Task Force, *Report to the 72nd Oregon Legislative Assembly on the Possible Alternatives to the Current System of Taxing Highway Use Through Motor Vehicle Fuel Taxes* (Salem, 2003), http://www.oregon.gov/ODOT/HWY/OIPP/docs/FinalReport2003march.pdf; James M. Whitty and Betsy Imholt, *Oregon's Mileage Fee Concept and Road User Fee Pilot Program, Report to the 73rd Oregon Legislative Assembly on Proposed Alternatives to the Current System of Taxing Highway Use Through Motor Vehicle Fuel Taxes*, (Salem, 2005), http://www.oregon.gov/ODOT/HWY/OIPP/docs/2005LegislativeReport.pdf; Oregon Department of Transportation," Road User Fee Task Force," http://www.oregon.gov/ODOT/HWY/OIPP/ruftf.shtml.

[151] Robert Salladay, "DMV Chief Backs Tax By Mile," *The Los Angeles Times*, November 16, 2004, home edition, sec. B.

to the owner.[152] A less invasive proposal is to add a device to the odometer.[153] Every time a driver pulls into a gas station, the device broadcasts the mileage, and the "use tax" is collected at the pump.[154]

2. PRIVACY CONCERNS

Even without any systems in use today, privacy experts fear secondary uses for the data and privacy invasions. As we have seen with other technologies, it seems likely that law enforcement, spurned spouses, insurance companies, and possibly marketing companies will all work to find ways to use the data for their own purposes.

IV. DISCUSSION

As we have shown, along with benefits from increasing technological sophistication in the automotive sphere, there are also privacy threats. A combination of the emerging technologies could create threats to privacy that are even worse than the dangers they pose on the individual level. For example, an insurance company with access to data from a system like OnStar will know when there has been an accident, and will be in a better position to request data from EDRs from mechanics. The combined data may lead to dropping a customer's insurance policy. Government surveillance can combine information from red light cameras' license plate recognition on local roads with E-ZPass highway data to track a person of interest very closely.

Most people do not consider privacy when they get into a car. Yet taken in aggregate, these technologies can report where you are, where you have traveled, who you have seen, and with whom you have traveled.

A. PRIVACY THREATS ASSOCIATED WITH EACH TECHNOLOGY

The table below summarizes the privacy threats associated with each technology discussed. Note that for "use taxes" this information is speculative, since the technology is still in the planning stage.

---

[152] Ibid.

[153] Ibid.

[154] Ibid.

Risk	*EDRs*	*Cameras*	*OnStar*	*GPS*	*E-Z Pass*	*Use Tax*
Technology can reduce safety		X	X	X		
Insurance company raises rates	X	X	X	X	X	X
Insurance company drops coverage	X	X	X	X		
Location data sold to marketing company			X			
Increased risk of criminal charges	X	X	X	X	X	X
Increased risk of tickets or fines		X		X	X	X
Data used in divorce proceedings		X	X	X	X	X
Parental surveillance of teens	X			X		
Government surveillance and data mining	X	X	X	X	X	X

1. TECHNOLOGY CAN REDUCE SAFETY

While most of the technologies listed are advertised as improving safety, in some cases they actually may decrease safety. As discussed in section III.B.3, red light cameras may increase traffic accidents, particularly rear-end collisions due to drivers slamming on the brakes. As discussed in section III.C.3, map systems that use GPS or OnStar may contribute to accidents by distracting drivers.

2. INSURANCE COMPANY RAISES RATES

Insurance companies are very interested in using new technologies to gain a competitive advantage in the way they set rates. As discussed in sections III.A.3 and III.A.4, insurance companies are exploring ways to charge rates based on mileage. EDRs that save speed and braking data for later retrieval, license plate recognition coupled with traffic cameras, OnStar data, GPS data, E-ZPass data, and highway use tax data are all useful in calculating mileage.

Insurance companies might be willing to purchase such data from state governments or obtain the data from an affiliated partner company like OnStar. As discussed in section III.A.3, insurance companies are also trying to amass a large database of EDR data to try to better predict which customers will have accidents.

3. INSURANCE COMPANY DROPS COVERAGE

Similarly, insurance companies may drop coverage for customers they believe represent high risks. For consumers, one advantage of insurance is to pool risk. For insurance companies, being able to exclude the most expensive customers allows greater profits or lower prices and thus greater market share. A person's insurance will probably not be dropped just for driving more miles than average, so E-ZPass and "use tax" data are not relevant. However, data that show drivers are aggressive in cornering (EDRs, OnStar), run red lights (traffic cameras), or even park in bad neighborhoods on a regular basis (GPS) are all potential flags for a higher risk policy. If insurance companies could combine data from these sources, they would have the ability to create better statistical models of which customers are likely to cost the most, and drop their coverage.

4. LOCATION DATA SOLD TO A MARKETING COMPANY

So far, the threat of marketing companies purchasing location based data is comparatively low. While marketing companies might welcome the opportunity to know which stores people visit, how long they visit any given store, and then tie that data to point of sale information to determine what they purchased, right now marketing companies do not have easy access to data. We include OnStar as a threat since, as discussed in section III.D.4, OnStar did offer a "virtual advisor" service that allowed real-time advertising for nearby products. EDRs do not record useful information for marketers. Marketers do not have access to affix GPS devices and transponders to hundreds of thousands of cars. At present, E-ZPass data only establishes which toll roads a customer takes. Marketers could install RFID readers in parking garages in order to track how frequently specific shoppers visit a given store, but the expense is prohibitive — and much of that data can be established by looking at credit card receipts. "use tax" data and traffic camera data might be interesting to marketers. That data is retained by various governments (both state and local), and some may be willing to sell it. So far, the threat of

sales to marketing companies is largely theoretical, but this is an area worth watching in the future.

5. INCREASED RISK OF CRIMINAL CHARGES

Increased risk of criminal charges is a major risk posed by new technologies. In particular, as discussed in section III.A.3, data can be used in court rooms to establish negligence, strict liability, or the defendant's failure to adhere to the reasonable person standard. EDRs have been used to determine speed and braking prior to a crash (section III.A.3). Red light cameras that have captured accidents and photos have been submitted as evidence (section III.B.3). OnStar reported a drunk driver to the police (section III.D.4). GPS was used in the Peterson murder trial (section III.C.4). The FBI cited availability of E-ZPass data as a reason to renew PATRIOT Act sunset provisions (section III.E.4). We assume the FBI would utilize "use tax" data similarly, since it provides even more information than E-ZPass. Note that these are examples of things that have already happened, rather than prospective threats. Law enforcement and the court system take full use of new technologies.

6. INCREASED RISK OF TICKETS OR FINES

Similarly, drivers are at an increased risk of traffic tickets or fines. EDRs have no way to tell what the speed limit is and it would be difficult to re-architect them for speeding tickets. Red light and speeding cameras are used to issue tickets — that is their primary purpose (section III.B.2). The risk from other technologies is low and largely theoretical. OnStar or GPS data could establish a driver's speed and location, then combine it with speed limit data to determine speeding. However, OnStar is unlikely to offer their data to law enforcement for speeding, as it would dramatically reduce their subscription base. Similarly, GPS is usually installed by vehicle owners, who are unlikely to purchase a system that reports them for speeding; parents may want to catch their children, but will not want to pay higher insurance and speeding tickets by sharing that data with law enforcement. E-ZPass and "use tax" proposals could very easily determine if a driver's average speed exceeded the limit. However, that doesn't appear to be happening currently.

7. DATA USED IN DIVORCE PROCEEDINGS

Divorces can become bitter, especially with large estates or child custody at stake. Private investigators attach concealed GPS devices to help establish infidelity (section III.C.4). Traffic cameras may capture unexpected passengers in photographs sent home to document running a red light or speeding, again giving rise to infidelity claims (section III.B.4). E-ZPass sends information home about time of day a car went through a toll booth, which may lead to suspicions. OnStar data is not readily available during a divorce, but may be subpoenaed from the company. We expect "use tax" data would be sent home like E-ZPass, but would include the fine detail of OnStar. While these threats to privacy do exist today, the majority of divorces do not involve suspicious spouses using covert means to spy on each other.

8. PARENTAL SURVEILLANCE OF TEENS

Parents not only watch each other, but they also watch their children. A commercial system warns teens not to brake too aggressively and logs the speeds recorded by the car's EDR (section III.B.3). Traffic cameras may show teens driving at times they were not allowed to drive, or in a car they were not supposed to operate (section III.B.4). OnStar, however, is not a likely source of data for parents. Some parents may elect to add GPS tracking to their cars, with or without their child's knowledge, and use that data to verify a child's location. As mentioned above, E-ZPass sends data home, and "use tax" would likely do the same. These technologies may also determine where a child traveled.

9. GOVERNMENT SURVEILLANCE AND DATA MINING

Government surveillance, in particular, receives a large boost from these new vehicular technologies. Now that it is economically and legally feasible to monitor large groups of people, law enforcement can track the movements of entire communities. Data can be stored indefinitely, allowing retroactive analysis. Data can be cross-checked to see which people gather together - who was in the parking lot for the ACLU meeting two years ago. Social networks can be studied - list everyone who parked within a three block range of John Smith's house on June 23rd. EDRs do not store data that is useful for government surveillance. However, traffic cameras, OnStar data, GPS devices attached by law enforcement, E-ZPass records, and "use tax"

data are all available to the government. This is another area where combining records allows a far more detailed picture than isolated data from one technology.

B. FAIR INFORMATION PRACTICE PRINCIPLES

Automotive privacy is not substantially different from other realms where privacy guidelines have been developed, and in some cases codified into law. The Organization for Economic Co-operation and Development ("OECD") Guide-lines on the Protection of Privacy and Transborder Data Flows of Personal Data are a useful framework for evaluating privacy.

The following table, which mirrors the analysis in Cranor's *I Didn't Buy It For Myself*,[155] gives an example of good behavior as well as how each of the eight OECD principles can be violated with automotive technologies.

OECD principles	*Good behavior*	*Potential violation*
Collection limitation	Do not collect more data than needed for the primary purpose.	Retaining "use tax" data with not just cumulative mileage, but also destination and travel path.
Data quality	Be clear on what level of accuracy to expect from tools.	A faulty EDR reading could result in an erroneous manslaughter conviction.
Purpose specification	State what data is used for.	Data from red light cameras was not supposed to be used to facilitate social network analysis.
Use limitation	Do not use data for new purposes without consent.	Mechanics give EDR data to insurance companies.
Security safeguards	Keep data safe and secure.	If hackers understand OnStar data, they can broadcast signals to open doors and start the ignition.

[155] Lorrie F. Cranor, "'I Didn't Buy it For Myself': Privacy and E-Commerce Personalization," 2004, http://lorrie.cranor.org/pubs/personalization-privacy.pdf.

Openness	Tell people when data is collected and what it is used for.	Not all states require notice for EDR systems.
Individual participation	Let people correct faulty data.	If a red light camera misidentifies a license plate number, it can be a nightmare to resolve.
Accountability	Be proactive in supporting these principles.	Lack of data retention policies allow these datasets to become targets for new uses and abuses.

Of particular concern is the lack of use limitations, which give rise to a multitude of secondary uses. While security has not yet been a major issue, we anticipate that it is just a matter of time before we read of a massive data breach. These dangers could be mitigated by following a policy of collection limitation.

C. POTENTIAL FOR CHANGE

We believe that the potential for surprise uses of data, as well as possible abuses of data, warrant changes to policies and practices at all levels. Who can create changes?

Actor	*Ability to influence change*
Insurance companies	While they have the power to simply not acquire data, the market will reward companies that exploit information advantages.
Car manufactures	Auto makers are in a position of power since they largely determine what goes into their cars at the factory. However, we do not anticipate benefits to car manufactures for a privacy protective stance, which makes it unlikely they will be concerned.
Consumers	Individuals can educate themselves and buy privacy friendly products. Yet in many cases, consumers have no real choices. EDRs and traffic cameras are ubiquitous. The only way to opt out of those privacy risks is to forgo driving, which is not a practical alternative in many areas.

Advocacy groups	Education and public awareness often precede changes. In many cases, educating legislative members about their personal privacy risks foster the enactment of better privacy protections for all citizens. We see an on-going role for advocacy.
Policy makers	New laws that curtail data use are the most likely path to increased privacy. At the Federal level, Congress can legislate the reach of the FBI and the PATRIOT Act to ensure new powers are used to fight terrorism, rather than as an expansive new set of surveillance powers used in a more indiscriminate way. At the state level, E-ZPass and "use tax" data can be restricted for the exclusive purpose of raising revenues. At the local level, traffic cameras can be deployed in ways that do not increase accidents, and the data can again be limited for use in traffic enforcement.

We have examined six automotive technologies: EDRs, traffic cameras, OnStar, GPS transponders, EZ-PASS, and "use tax" proposals. These are powerful tools and technologies. Used with care and restraint, they may prove beneficial. However, technology is developing without concern for consumer privacy. Every one of the technologies we examined violates the Fair Information Practices. Ubiquitous use of privacy invasive technology as part of every-day life is likely to create a chilling effect. These issues cut to the core of the right to assembly and the ability to dissent in a democracy.

In the short term, it is unlikely that car manufacturers and insurance companies will see consumer privacy as anything but a barrier to profits. Advocacy groups may educate consumers, who can in turn put pressure on corporations to change their practices. This probably will not happen soon, yet advances in technologies do happen quickly.

We hope that moving forward, policy makers will turn their attention to privacy issues and act in ways that protect their constituents. It is often easier to enact legislation prior to new systems and to "build in" privacy. For example, the new "use tax" proposals can be implemented in privacy protective ways that also support raising revenues. However, it is not too late to add privacy protections after technology is widely deployed, as we see with new laws around EDR data. In this way we can gain the benefits of new technologies without also incurring unfortunate side effects.